Daily brief, Wednesday, February 18, 2026

Feb 17, 7:00 PM to Feb 18, 7:00 PM ET

Generated Nov 7, 2026, 4:52 PM ET

0	2	0	21	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 21 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

10.0 **CVE-2026-22769** Dell RecoverPoint for Virtual Machines (RP4VMs) CISA KEV

Unauthenticated remote attackers gain root-level OS access and persistence in Dell RecoverPoint for Virtual Machines (RP4VMs) via hard-coded credentials.

6.8 **CVE-2021-22175** GitLab GitLab CISA KEV DETECTION

An attacker gains unauthorized access to internal services and data in GitLab through a server-side request forgery flaw in URL handling.

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs

21

10.0 **CVE-2026-22769** Dell RecoverPoint for Virtual Machines (RP4VMs) KEV

Unauthenticated remote attackers gain root-level OS access and persistence in Dell RecoverPoint for Virtual Machines (RP4VMs) via hard-coded credentials.

9.0 **CVE-2026-0573** GitHub enterprise server

An URL redirection vulnerability was identified in GitHub Enterprise Server that allowed attacker-controlled redirects to leak sensitive authorization tokens. The repository_pages API insecurely followed HTTP redirects when fetching artifact URLs, preserving t

9.8 **CVE-2026-2329** Grandstream gxp1610 firmware

An unauthenticated stack-based buffer overflow vulnerability exists in the HTTP API endpoint /cgi-bin/api.values.get. A remote attacker can leverage this vulnerability to achieve unauthenticated remote code execution (RCE) with root privileges on a target devi

9.8 **CVE-2026-27175** Mjdm majordomo

MajorDoMo (aka Major Domestic Module) is vulnerable to unauthenticated OS command injection via rc/index.php. The $param variable from user input is interpolated into a command string within double quotes without sanitization via escapeshellarg(). The command

9.8 **CVE-2026-27174** Mjdm majordomo DETECTION

MajorDoMo (aka Major Domestic Module) allows unauthenticated remote code execution via the admin panel's PHP console feature. An include order bug in modules/panel.class.php causes execution to continue past a redirect() call that lacks an exit statement, allo

9.8 **CVE-2025-65791** Zoneminder zoneminder

ZoneMinder v1.36.34 is vulnerable to Command Injection in web/views/image.php. The application passes unsanitized user input directly to the exec() function. NOTE: this is disputed by the Supplier because there is no unsanitized user input to web/views/image.p

9.8 **CVE-2026-27180** Mjdm majordomo

MajorDoMo (aka Major Domestic Module) is vulnerable to unauthenticated remote code execution through supply chain compromise via update URL poisoning. The saverestore module exposes its admin() method through the /objects/?module=saverestore endpoint without a

9.8 **CVE-2019-25364** Tabslab mailcarrier

MailCarrier 2.51 contains a buffer overflow vulnerability in the POP3 USER command that allows remote attackers to execute arbitrary code. Attackers can send a crafted oversized buffer to the POP3 service, overwriting memory and potentially gaining remote syst

9.1 **CVE-2026-25548** Invoiceplane invoiceplane

InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A critical Remote Code Execution (RCE) vulnerability exists in InvoicePlane 1.7.0 through a chained Local File Inclusion (LFI) and Log Poisoning attack. An auth

9.8 **CVE-2019-25360** Aida64 aida64

Aida64 Engineer 6.10.5200 contains a buffer overflow vulnerability in the CSV logging configuration that allows attackers to execute malicious code by crafting a specially designed payload. Attackers can exploit the vulnerability by creating a malformed log fi

9.4 **CVE-2025-70141** Oretnom23 customer support system

SourceCodester Customer Support System 1.0 contains an incorrect access control vulnerability in ajax.php. The AJAX dispatcher does not enforce authentication or authorization before invoking administrative methods in admin_class.php based on the action parame

9.8 **CVE-2019-25362** Alloksoft wmv to avi mpeg dvd wmv convertor

WMV to AVI MPEG DVD WMV Convertor 4.6.1217 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting the license name and license code fields. Attackers can craft a malicious payload of 6000 bytes to trigger a bind

9.8 **CVE-2019-25361**

Ayukov NFTP client 1.71 contains a buffer overflow vulnerability in the SYST command handling that allows remote attackers to execute arbitrary code. Attackers can send a specially crafted SYST command with oversized payload to trigger a buffer overflow and ex

9.8 **CVE-2025-70150** Codeastro membership management system

CodeAstro Membership Management System 1.0 contains a missing authentication vulnerability in delete_members.php that allows unauthenticated attackers to delete arbitrary member records via the id parameter.

9.1 **CVE-2025-70146** Projectworlds online time table generator

Missing authentication in multiple administrative action scripts under /admin/ in ProjectWorlds Online Time Table Generator 1.0 allows remote attackers to perform unauthorized administrative operations (e.g.,adding records, deleting records) via direct HTTP re

9.8 **CVE-2019-25365**

ChaosPro 2.0 contains a buffer overflow vulnerability in the configuration file path handling that allows attackers to execute arbitrary code by overwriting the Structured Exception Handler. Attackers can craft a malicious configuration file with carefully con

9.8 **CVE-2025-70152** Fabian scholars tracking system

code-projects Community Project Scholars Tracking System 1.0 is vulnerable to SQL Injection in the admin user management endpoints /admin/save_user.php and /admin/update_user.php. These endpoints lack authentication checks and directly concatenate user-supplie

9.8 **CVE-2025-70998** Utt 810 firmware

UTT HiPER 810 / nv810v4 router firmware v1.5.0-140603 was discovered to contain insecure default credentials for the telnet service, possibly allowing a remote attacker to gain root access via a crafted script.

9.8 **CVE-2025-70149** Codeastro membership management system

CodeAstro Membership Management System 1.0 is vulnerable to SQL Injection in print_membership_card.php via the ID parameter.

9.5 **CVE-2025-15579**

Deserialization of Untrusted Data vulnerability in OpenText™ Directory Services allows Object Injection. The vulnerability could lead to remote code execution, denial of service, or privilege escalation. This issue affects Directory Services: before 24.4.16, f

1 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Figure figure.com FINANCE 967,178 accounts

Watch Floor collects CVE records, CISA KEV, exploit indexes, official advisories, security news and chatter. CVSS is the headline score. Ransomware posts are criminal groups' claims, not confirmed by the victims. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.